

# AMP FOR ENDPOINTS RELEASE NOTES

Version 5.4

16 April 2021

## AMP for Endpoints Mac Connector 1.15.3

### Bugfixes/Enhancements

- Fixed an issue where the Connector no longer recognizes macOS binaries as signed with a trusted certificate, resulting in increased CPU usage and possible Time Machine failures on the endpoint. (CSCvy01803)

14 April 2021

## AMP for Endpoints Console 5.4.20210414

### Bugfixes/Enhancements

- Event filtering updated to include Behavioral Protection URL and registry observable data.
- Login credentials are no longer required for Windows scheduled scans and endpoint IOC scans.
- Fixed a bug that caused an erroneous message about iOS devices when moving computers to a new group.
- Added a warning on policies when engines are disabled or in audit mode.
- Interface and usability improvements to various pages.

31 March 2021

### AMP for Endpoints Console 5.4.20210331

#### Bugfixes/Enhancements

- Fixed a rendering issue on the dashboard when the SecureX ribbon is enabled.
- Fixed preset policies to match recommended settings.
- Fixed a formatting issue in SecureX threat hunting reports.

30 March 2021

### AMP for Endpoints Windows Connector 7.3.15

#### Bugfixes/Enhancements

- Behavioral Protection no longer causes high single core CPU usage when disabled. (CSCvx41502)
- Stability updates for Exploit Prevention.
- Addressed vulnerability described in CVE-2021-1386. (CSCvw77090)
- Fixed Exploit Prevention engine compatibility issues with the following applications:
  - Firefox (CSCvx49567)
  - Powershell (CSCvx47570)
  - Lenovo Smart Standby (CSCvx54732)
  - Microsoft Control Flow Enforcement (CET)
  - Cortex XDR
  - Office Plus
  - Thinapp

17 March 2021

### AMP for Endpoints Console 5.4.20210317

#### New

- Users can now enable and disable the file fetch from the Features section of the Organization Settings page.
- Added a feedback form to capture user comments and bug reports.

### Bugfixes/Enhancements

- Fixed an issue where links to unseen devices on the iOS Clarity dashboard tab were not working correctly.

15 March 2021

## AMP for Endpoints Linux Connector 1.15.2

### Bugfixes/Enhancements

- Added support for wildcards in process exclusions.
- Fixed an issue where some rename operations would not trigger an on-access scan on RHEL 7/8 and Ubuntu 20.04 LTS.
- Fixed a memory leak that could occur due to a specific mount configuration on the endpoint. (CSCvx34973)
- Added new command for checking Connector posture to ampcli.
- Added new command for getting status help to ampcli.
- The Connector will now raise fault 16 if it is not compatible with the currently running kernel.
- Fixed an issue where the Ubuntu Connector install package would always overwrite the policy file if one already existed on the computer.
- Updated ClamAV to 0.103.1.

## AMP for Endpoints Mac Connector 1.15.2

### New

- The Connector now runs on ARM architecture without Rosetta emulation. See [AMP for Endpoints Mac Connector OS Compatibility](#) for more information.

---

**IMPORTANT!** Version 1.15.2 has a larger install package than previous releases. Customers affected by CSCv37020 on Connector versions 1.12.6 or older should upgrade to an intermediate Connector version (1.12.7-1.15.1) before upgrading to version 1.15.2.

---

### Bugfixes/Enhancements

- Added support for wildcards in process exclusions.
- Fixed an issue where the Connector was not sending Execution Blocked events in active mode for programs executing in deep directories.
- Fixed a memory leak when running on macOS 11 that can occur when on-execute mode is set to active in policy.
- Improved URL flow visibility for HTTPS and HTTP/3 protocols on macOS 11.
- Added new command for checking Connector posture to ampcli.

3 March 2021

- Added new command for getting status help to ampcli.
- Updated ClamAV to 0.103.1.

3 March 2021

## AMP for Endpoints Console 5.4.20210303

### Bugfixes/Enhancements

- Minor bugfixes and performance enhancements.

23 February 2021

## AMP for Endpoints Android Connector 2.1.0.14

### New

- Added support for assigning device names and bootstrap URLs through an MDM.
- New status page for viewing device information.

### Bugfixes/Enhancements

- More robust auto-scanning of apps.
- Support for scanning apps with multiple split apks.
- Enhancements to Activity Log to show recently scanned apps.
- Fixed a bug where logs were not being exported on devices running Android 10 and above.
- Improved error handling.
- Improved logging for troubleshooting.
- Other bug fixes and UI enhancements.

16 February 2021

## AMP for Endpoints Console 5.4.20210216

### Bugfixes/Enhancements

- Improved conviction settings for the script control engine in Windows policies.
- Added controls to quickly apply recommended workstation and server settings for modes and engines in Windows policies.
- Conviction modes for new Windows policies now default to the recommended workstation settings.

4 February 2021

- Added descriptions for each engine's conviction mode settings.
- Improved contextual help throughout policy edit pages.
- Updated Advanced Custom Detection signature validation to stop errors when uploading custom clamAV signatures.

4 February 2021

## AMP for Endpoints Windows Connector 7.3.13

### New

- The Connector files will only be signed with a SHA-2 certificate and no longer be signed with a SHA-1 certificate starting with this release.
- Behavioral Protection now monitors processes making outgoing HTTP calls for malicious activity.

### Bugfixes/Enhancements

- Made performance and stability improvements to the Exploit Prevention engine.
- Improved the stability of the Device Flow Correlation engine and driver.
- Addressed a potential hang on Connector shutdown.
- Addressed an issue where in rare cases the Behavioral Protection engine could cause a blue screen.
- The Behavioral Protection engine now properly monitors file deletes on FAT32 file systems.
- Improved quarantine process for files that are signed with both a SHA-1 and SHA-2 certificate.
- Resolved Exploit Prevention engine compatibility issues with SKYSEA client. (CSCvx02971)
- Addressed an issue where the Orbital service might start while disabled in policy. (CSCvw65300)

2 February 2021

## AMP for Endpoints Console 5.4.20210202

### Bugfixes/Enhancements

- Added a button in Device Trajectory to return to a selected event in the timeline if you scroll away from it.
- Removed a file from default Script Control rules to address false positives.
- Fixed a timestamp issue with low prevalence executables that was causing errors when generating reports.

28 January 2021

## AMP for Endpoints Mac Connector 1.15.1

### Bugfixes/Enhancements

- Fixed a bug where the AMP Security Extension was incorrectly translated into Korean in the System Preference Full Disk Access window.
- Fixed a memory growth issue when monitoring connections made with Apple's NSURL API with macOS System Extensions. (CSCvx09259)

26 January 2021

## AMP for Endpoints Linux Connector 1.15.1

### New

- Added official support for Ubuntu 20.04.0 LTS and 20.04.1 LTS. See [AMP for Endpoints Linux Connector OS Compatibility](#) for supported operating systems and kernel versions.

### Bugfixes/Enhancements

- The Connector will now raise fault 5, amp-scan-svc-user unavailable if its directory privileges have been revoked.
- Added patches for libxml2 version 2.9.10 to address the vulnerability described in CVE-2020-7595.

19 January 2021

## AMP for Endpoints Console 5.4.20210119

### Bugfixes/Enhancements

- Endpoint IOC scheduled scan times are now displayed without a time zone on the scan summary page because scans start in the Connector local time zone.
- Filtering by the statistics at the top of the Computers page now stacks the filters when clicking each one instead of clearing the previous filtered view.
- You can now opt the entire organization out of Google Analytics on the Organization Settings page.
- Added the IP pivot menu to the Audit page.
- Links to Related Events on the Inbox page now go to the new Device Trajectory view.

7 January 2021

- Added Connector scan requests to audit logs.
- Fixed style and alignment issues on various pages.

7 January 2021

## AMP for Endpoints Console 5.4.20210107

### Bugfixes/Enhancements

- Minor bugfixes and performance enhancements.

## Archived release notes

Previous years release notes can be found at the following links:

- [2020 release notes](#)
- [2019 release notes](#)
- [2018 release notes](#)
- [2017 release notes](#)
- [2016 release notes](#)
- [2015 release notes](#)
- [2014 release notes](#)
- [2013 release notes](#)